FORM PTO-1390 (REV. 5-93)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER **2345/62**

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
To be assigned 09/269830

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP97/05081	**17 September 1997 (17.09.97)**	**01 October 1996 (01.10.96)**

TITLE OF INVENTION
METHOD OF TRANSMITTING SIGNALS

APPLICANTS FOR DO/EO/US SCHEERHORN, Alfred and HUBER, Klaus

Applicants herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: First page of published application, International Search Report and PCT/RO/101 Request Form.

74586-1
Express Mail No. EL169614947US

U S APPLICATION NO. if known, see 37 C F R.1 5	INTERNATIONAL APPLICATION NO PCT/EP97/05081	ATTORNEY'S DOCKET NUMBER 2345/62

17. ☒ The following fees are submitted:

CALCULATIONS ! PTO USE ONLY

Basic National Fee (37 CFR 1.492(a)(1)-(5)):
Search Report has been prepared by the EPO or JPO . . . . . ~~$930~~ 840.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) . $720.00

No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $790.00

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1,070.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $98.00

ENTER APPROPRIATE BASIC FEE AMOUNT =				$ ~~930~~ 840.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$ 0	
Claims	Number Filed	Number Extra	Rate		
Total Claims	13 - 20 =	0	X $18.00	$ 0	
Independent Claims	1	0	X $78 00	$ 0	
Multiple dependent claim(s) (if applicable)			+ $260.00	$ 0	
*based on Preliminary Amendment		TOTAL OF ABOVE CALCULATIONS =		$ ~~930~~ 840.00	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$ 0	
		SUBTOTAL =		$ ~~930~~ 840.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).			+	$ 0	
		TOTAL NATIONAL FEE =		$ ~~930~~ 840.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property			+	$ 0	
		TOTAL FEES ENCLOSED =		$ ~~930~~ 840.00	
*Calculations based on Preliminary Amendment.				Amount to be: refunded	$
				charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of **$~~930~~ 840.00** to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Richard L. Mayer (Reg. No. 22,490)

DATE 4/1/98

KENYON & KENYON
One Broadway
New York, NY 10004

[2345/62]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: SCHEERHORN ET AL.

SERIAL NO.: to be assigned

FILED: herewith

TITLE: SIGNAL TRANSMISSION PROCESS

ART UNIT: not yet known

EXAMINER: not yet known

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT

Please amend the above-identified application before a first consideration on the merits as follows:

IN THE TITLE

Please change the title to --METHOD OF TRANSMITTING SIGNALS--.

IN THE SPECIFICATION

On page 1, before line 1, insert --Field of the Invention--.

On page 1, line 1, change "according to the" to --between a transmitter and a receiver using keys and cryptographic algorithms--.

On page 1, delete line 2.

On page 1, before line 4, insert --Related Technology--.

On page 1, line 27, change "but" to --because--.

On page 2, before line 5, insert --Summary of the Invention--.

On page 2, line 5, change "the object" to --an object-- and change "create" to --provide--.

EL169614947 US

On page 2, line 9, change "transmission" to --communication--.

On page 2, delete lines 11-16.

On page 2, before line 18, insert --The present invention provides a method for transmitting signals between a transmitter and a receiver, the method comprising calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase, and calculating authentication tokens for the signals as a function of the data, in a communication phase, so as to authenticate both the signals and a transmission sequence of the signals.--

On page 2, line 22, change "already" to --previously-- and change "The desired object is achieved" to --A method according to the present invention--.

On page 2, line 23, change "by a method composed of" to --includes--.

On page 3, before line 19, insert--Brief Description of the Drawings--.

On page 3, line 20, change "drawing" to --drawings-- and change "which shows" to --in which--.

On page 3, line 22, between "Figure 1" and "a" insert --shows-- and change "the receiver," to --a receiver;--.

On page 3, line 24, between "Figure 2" and "a" insert --shows--.

On page 3, before line 26, insert --Detailed Description--.

On page 3, line 26, change "This method" to --A method according to the present invention--.

On page 4, line 1, change "Using the" to --Using a--.

On page 4, line 8, change "M" to --m--.

On page 5, line 27, change "With" to --For--.

On page 5, line 28, change "possible" to --sufficient-- and delete "with no".

On page 5, delete line 29.

On page 7, line 17, change "s[w]+t[i]" to --s[w]⊕t[i]--.

On page 9, line 1, change "Patent Claims" to --WHAT IS CLAIMED IS:--.

IN THE CLAIMS

Please cancel claims 1-10 and the new (revised) patent claims 1, 2, 5, 8 and 9, and add new claims 11-23 as follows:

--11. (new) A method for transmitting signals between a transmitter and a receiver, the method comprising:

calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase; and

calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and a transmission sequence of the signals.

12. (new) The method as recited in claim 11 wherein the calculation phase includes generating a pseudo-random sequence.

13. (new) The method as recited in claim 12 wherein certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence, and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of the coding of the signal and the coding of the respective position in the transmission sequence.

14. (new) The method as recited in claim 13 wherein the authentication token of the one signal transmitted at the i-th position is a bit-by-bit XOR link or an equivalent logic function of the coding of the one signal and the coding of the respective position in the transmission sequence.

15. (new) The method as recited in claim 11 wherein the calculation phase includes generating a pseudo-random sequence.

16. (new) The method as recited in claim 15 wherein certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence, and wherein the authentication token of a one of the signals transmitted at an i-th position is calculated as a function of the coding of all previously transmitted signals and the coding of the respective position in the transmission sequence.

17. (new) The method as recited in claim 16 wherein the authentication token of the one signal transmitted at the i-th position is a bit-by-bit XOR link or an equivalent logic link of the coding of all the previously transmitted signals and the coding of the respective position in the transmission sequence.

18. (new) The method as recited in claim 11 wherein the at least one cryptographic algorithm includes a block cipher.

19. (new) The method as recited in claim 18 wherein the block cipher includes a data encryption standard.

20. (new) The method as recited in claim 12 wherein the at least one cryptographic algorithm includes a block cipher, the pseudo-random sequence being generated by operating the block cipher in a known output feedback mode.

21. (new) The method as recited in claim 15 wherein the at least one cryptographic algorithm includes a block cipher, the pseudo-random sequence being generated by operating the block cipher in a known output feedback mode.

22. (new) The method as recited in claim 11 wherein the communication phase further includes calculating another token for authentication of the transmitter, the other token being subsequently transmitted so as to initialize the receiver for authentication of the transmitter.

23. (new) The method as recited in claim 11 further comprising confirming the transmission sequences by nonintersecting m-bit strings.--

REMARKS

This Preliminary Amendment cancels original claims 1-10 in the underlying PCT Application No. PCT/EP97/05081, and adds new claims 11-23. The new claims do not add new matter to the application but do conform the claims to U.S. Patent and Trademark Office rules.

The amendments to the specification are to conform the specification to U.S. Patent and Trademark Office rules and do not introduce new matter into the application.

The underlying PCT application includes a Search Report (copy included).

Conclusion

Consideration of the present application as amended is hereby respectfully requested.

Respectfully Submitted,

Kenyon & Kenyon

Dated: 29 March 1999

By: Erik R. Swanson

Erik R. Swanson
(Reg. No. 40,833)

One Broadway
New York, NY 10004
(212) 425-7200

[2345/62]

SIGNAL TRANSMISSION PROCESS

The present invention relates to a method of transmitting signals according to the definition of the species of Patent Claim 1.

In transmission of signal sequences, authentic transmission of the data or signals always plays a major role. For example, one method of achieving this goal is described in ISO/IEC 9797, Information Technology - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm (JTC1/SC27 1994). Identical secret keys in combination with an encoding algorithm (block cipher, encipherment algorithm) or with a key-dependent single-way function (cryptographic check function) are assigned to the transmitter and the receiver. This can take place, for example, on a card. The transmitter adds a cryptographic check sum (message authentication code) to each signal (datum) depending on the secret key and the cryptographic algorithm (encoding or single-way function). The receiver in turn calculates the check sum and acknowledges the received signals as authentic if the check sum is identical. However, this method has the following disadvantages: to detect a change in sequence of transmitted data, the check sum of a signal is calculated as a function of the check sum of the signals transmitted previously. Even in the case when a check sum is transmitted after each signal, this is still necessary because otherwise a hacker could record pairs of signal check sums and enter them in an altered sequence without being detected. With the known method, this requires the cryptographic algorithm to be executed for each check sum. Since the sequence and selection of signals are not precisely fixed in advance, it is impossible to calculate the required check sums in advance.

This can lead to problems in a time-critical environment. The cryptographic algorithm can be calculated on a chip card, for example. This is advantageous when using a chip card that has already been evaluated, but otherwise an additional software

achieved by a method composed of a preliminary calculation phase and a communication phase in which the signals or data are transmitted together with the check sums. In the preliminary calculation phase, first a pseudo-random sequence Z is generated by cryptographic algorithms, e.g., a block cipher in the output feedback mode, from the time-variant parameter (sequence number, time mark and other initialization data). As an example, m = 16, 32 or 64 is assumed for a security parameter m. Then nonintersecting strings z(i) of m bits each from sequence Z are assigned to signals s[i], i = 1, 2, ..., n of the signal supply. Additional nonintersecting m-bit strings t[i] are selected from the remaining sequence as the coding of numbers 1, 2, ... MAX, where MAX is the maximum number of signals to be transmitted.

If transmitter authentication is necessary in the subsequent communication phase, then first the sequence of one pass authentication is performed according to the publications ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) and ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995). The transmitter transmits the initialization information and the time-variant parameters to the receiver, and it transmits a number of previously unused bits from Z to the receiver as an authentication token. The receiver in turn calculates pseudo-random sequence Z and checks the received authentication token. The signals received by the receiver during the signal transmission are accepted as authentic if the received authentication token matches the token calculated. In addition, modifications of this method are also possible, as described in detail in the following specification.

The present invention will now be described in greater detail on the basis of embodiments illustrated in the drawing, which shows:

Figure 1 a flow chart for the schematic operation sequence in the receiver, and

Figure 2 a flow chart for the schematic operation sequence in a transmitter.

This method includes a preliminary calculation phase and a communication phase in which the signals are transmitted together with the check sums.

Preliminary calculation phase:

Using the cryptographic algorithm (for example, a block cipher in the output feedback mode according to ISO/IEC 10116, Information Processing - Modes of operation for an n-bit block cipher algorithm (JTC1/SC27 1991)), first a pseudo-random sequence Z is generated from a time-variant parameter (sequence number, time mark, according to ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994)) and other initialization data. Let m be a security parameter, such as M [sic] = 16, 32 or 64. Then from the sequence Z, nonintersecting strings z[i] with m bits each are assigned to signals s(i), i = 1, 2, ..., n of the signal supply. From ...

the authentication token received by the transmitter matches the token calculated.

The sequence of transmitted signals is guaranteed by the influence of the values t[i].

One variant of signal authentication proceeds as follows: If it is necessary to select authentication token T(i) of the i-th signal s[k[i-1]] as a function of all previously transmitted signals s[k[1]], ..., s[k[i-1]], then the token

T(i) = f(t[i], F(i)) can be transmitted for authentication of the i-th signal s[k[i]], where

F(1) = s[k[1]] and

F(i) = f(s[k[i]], F(i-1)) for i > 1.

Calculation of authentication token T(i) thus requires calculation of f twice.

One example of using such a method is the authentic establishment of a connection in making a telephone call. When transmitting the dial tones, it is not known whether an additional dial tone will follow. Therefore, it seems necessary to authenticate each dial tone by transmitting a token in the pause following it. With multi-frequency dialing methods, the length of the dial tones is at least 65 ms, and the length of the pause between dial tones is at least 80 ms. For the authentication described here, this short interval of 145 ms for authentication is sufficient with no problem.

First, the sequence of operations or steps by the receiver are described on the basis of a flow chart according to Figure 1.

In the telephone example, the transmitter is the telephone, optionally equipped with a cryptographic module and/or ...

s[max] = bit (smax-1)*m+1 through bit smax*m of random sequence PRS

t[1] = bit smax*m+1 through bit (smax+1)*m of random sequence PRS

...

t[tmax] = bit (smax+tmax-1)*m+1 through bit (smax+tmax)*m of random sequence PRS

The sequence of operations or steps for the transmitter is described below on the basis of Figure 2.

S3: The transmitter waits for a signal w which is to be transmitted authentically; w is interpreted as a natural number between 1, 2, ..., smax in order to keep the mapping w -> s[w] simple.

S4: The transmitter sends the I-th signal w together with authentication token f(s[w], t[i]). In the telephone example, the token is f(s[w], t[i]) = s[w]⊕t[i], the bit-by-bit XOR of s[w] and t[i].

S5: S3 and S4 are iterated either until no more signals are to be transmitted authentically or until the maximum number of signals that can be authenticated with this supply of previously calculated random sequence PRS has been reached.

S6: In the telephone example, the transmitter is now waiting for a connection to be established with the receiver.

E3, E4 and E5: As long as new signals with the respective authentication tokens are received, the receiver checks on whether the authentication tokens calculated by it match the received tokens.

First, the sequence of operations or steps by the receiver are described on the basis of a flow chart according to Figure 1.

In the telephone example, the transmitter is the telephone, optionally equipped with a cryptographic module and/or chip card, and the receiver is the telephone network, such as the closest exchange.

E1 and S1: The time-invariant parameter here is synchronized between the receiver and transmitter. The time-invariant parameter may be a sequence number or a time mark which has been synchronized. This parameter may optionally also be transmitted as plain text or in encoded form from the transmitter to the receiver for synchronization. In the method according to the present invention, it is expedient that the transmitter already knows the time-invariant parameter before a connection is attempted in order to calculate s[], t[] in advance.

E2 and S2: The transmitter and receiver here first calculate a random sequence PRS (pseudo-random sequence) of length m* (smax + tmax) bits, where

m: security parameter, namely in this example m: = 32.

smax: Maximum number of different signals (number of elements of the alphabets/signal supply). In the telephone example, this refers to digits 1 through 9 and special symbols such as # and others.

tmax: Maximum number of signals to be authenticated in one pass. In the telephone example this would be the maximum length of a telephone number, the maximum number of digits and special symbols for establishing a connection.

Then nonintersecting strings of m bits of this random sequence PRS are assigned to m-bit quantities s[1], s[2], ..., s[smax], t[1], t[2], ..., t[tmax], etc.

s[1] = bit 1 through bit m of the PRS

s[2] = bit m+1 through bit 2*m of the PRS

...

s[max] = bit (smax-1)*m+1 through bit smax*m of random sequence PRS

t[1] = bit smax*m+1 through bit (smax+1)*m of random sequence PRS

t[tmax] = bit (smax+tmax-1)*m+1 through bit (smax+tmax)*m of random sequence PRS

The sequence of operations or steps for the transmitter is described below on the basis of Figure 2.

S3: The transmitter waits for signal w which is to be transmitted authentically; w is interpreted as a natural number between 1, 2, ..., smax in order to keep the mapping w -> s[w] simple.

S4: The transmitter sends the I-th signal w together with authentication token f(s[w], t[i]). In the telephone example, the token is f(s[w], t[i]) = s[w]+t[i], the bit-by-bit XOR link of s[w] and t[i].

S5: S3 and S4 are iterated either until no more signals are to be transmitted authentically or until the maximum number of signals that can be authenticated with this supply of previously calculated random sequence PRS has been reached.

S6: In the telephone example, the transmitter is now waiting for a connection to be established with the receiver.

E3, E4 and E5: As long as new signals with the respective authentication tokens are received, the receiver checks on whether the authentication tokens calculated by it match the received tokens.

E6: If all the tokens match, the received signals are accepted as authentic. In the telephone example, the connection is now established.

E7: If authentication is unsuccessful, no connection is established.

Patent Claims

1. A method of transmitting signal/data sequences between a transmitter and a receiver with authentication of the transmitted signal/data sequences by using keys and cryptographic algorithms, which are implemented on the transmitter end as well as on the receiver end, characterized in that
in a preliminary calculation phase, data is calculated as a function of a secret key using cryptographic algorithms, and then in a subsequent transmission phase, authentication tokens for the signals are calculated from this data, authenticating both the signals as well as the sequence in which the signals are transmitted.

2. The method according to Patent Claim 1, characterized in that
in a preparatory phase, a pseudo-random sequence (PRS) is generated using a cryptographic algorithm;
certain strings of this sequence are used as a code for the signals of the signal supply as well as the transmitting stations (1, 2, ... MAX); and
the authentication token of the signal transmitted at the i-th (i = 1, 2, ..., MAX) position is calculated as a function of the coding of the signal and the coding of the transmission position (i).

3. The method according to Patent Claim 2, characterized in that
the authentication token (T) of the signal transmitted at the i-th position (i = 1, 2, ..., MAX) is the bit-by-bit XOR link or an equivalent logic function of the coding of the respective signal and the coding of the transmission position (i).

4. The method according to Patent Claim 1, characterized in that
a pseudo-random sequence (PRS) is generated in the preliminary calculation phase using a cryptographic algorithm;
certain strings of this sequence are used as the coding of the signals of the

signal supply as well as the transmitting stations (1, 2, ..., MAX); and
the authentication token of the signal transmitted at the i-th position (i = 1, 2, ..., MAX) is calculated as a function of the coding of all the previously transmitted signals (1, 2, ..., i) and of the coding of the transmission position (i).

5. The method according to one of Patent Claims 1 through 4, characterized in that
the authentication token (T) of the signal transmitted at the i-th position (i = 1, 2, ... MAX) is the bit-by-bit XOR link or an equivalent logic link of the coding of all previously transmitted signals (1, 2, ... i) and the coding of the transmission position (i).

6. The method according to one of Patent Claims 1 through 5, characterized in that
the cryptographic algorithm used in the preliminary calculation phase is a block cipher.

7. The method according to Patent Claim 6, characterized in that
the known data encryption standard is used as the block cipher.

8. The method according to one of Patent Claims 6 or 7, characterized in that
the pseudo-random sequence (PRS) is generated by operating the block cipher in the known output feedback mode.

9. The method according to the definition of the species of Patent Claim 1 or according to one of Patent Claims 2 through 8, characterized in that
a token (T) for authentication of the respective transmitter is also calculated in the preparatory phase and is transmitted subsequently, initializing the receiver for authentication of the transmitter.

10. The method according to one of Patent Claims 1 through 9, characterized in that

the sequence of the transmitted signals is confirmed by nonintersecting m-bit strings (t(i)).

Abstract

A process for transmitting sequences of signals/data from a transmitter to a receiver and for authenticating the sequences of signals/data consists of a precalculation phase and of a communication phase in which the signals are transmitted together with the checking sums. In the precalculation phase, a pseudo-random sequence is first generated by means of a cryptographic algorithm from a time-variable parameter and other initialization data. Non-overlapping sections (z(1) of a sequence (z) having each m bits are associated to signals (s(i)), wherein i = 1, 2, ... n, of a signal storage. Further non-overlapping m bit sections (t(i)) of the remaining sequence are selected for coding numbers (1, 2, ... MAX). The transmitter transmits the initialisation information and the time-variable parameters to the receiver and the receiver calculates the pseudo-random sequence (Z) and checks the received authentication token (T). The transmitter accepts the received signals as being authentic when the received authentication tokens match the calculated ones.

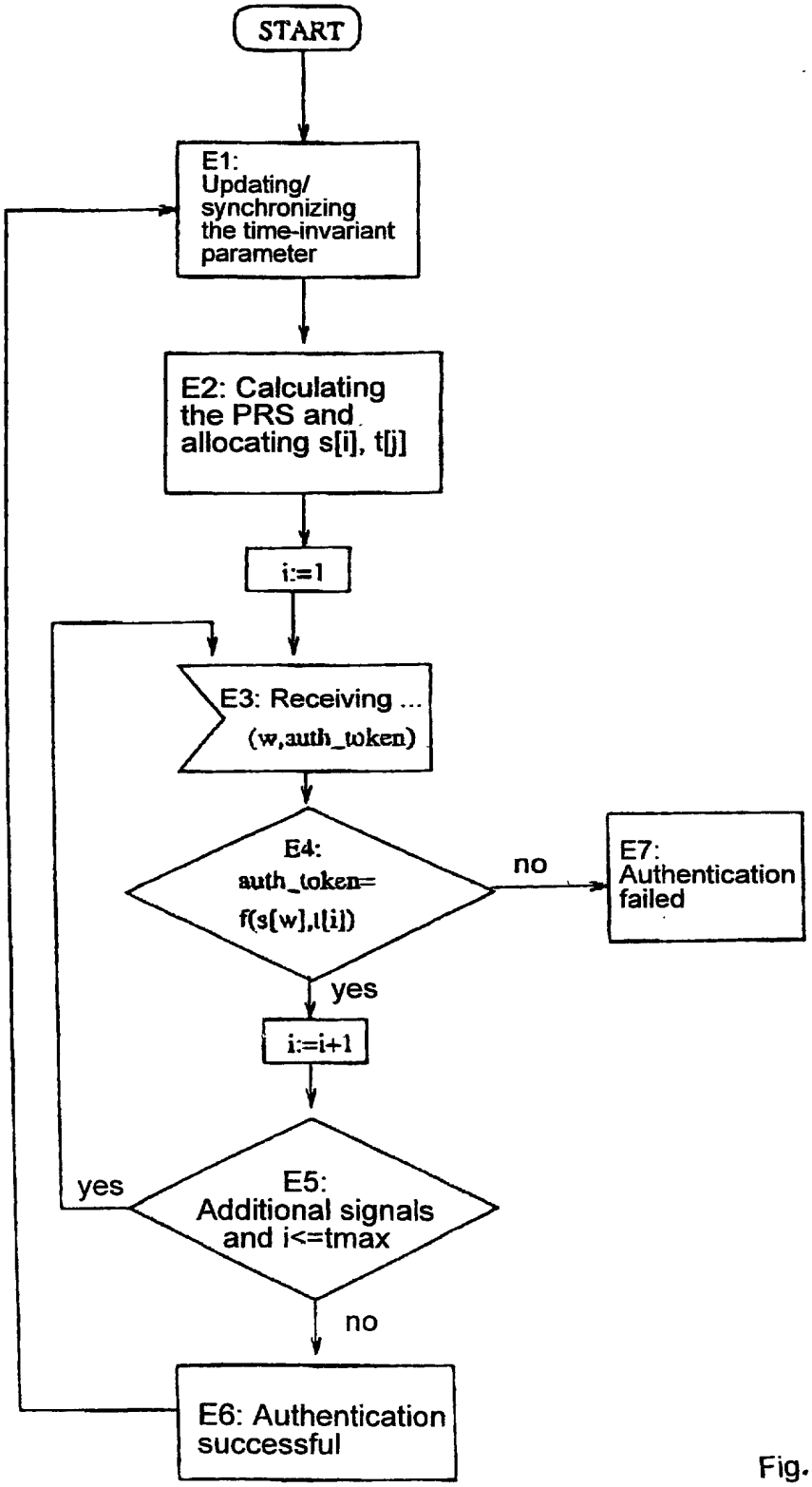
START
E1: Updating/ synchronizing the time-invariant parameter
E2: Calculating the PRS and allocating s[i], t[j]
i:=1
E3: Receiving ... (w,auth_token)
E4: auth_token= f(s[w],t[i])
no
E7: Authentication failed
yes
i:=i+1
E5: Additional signals and i<=tmax
yes
no
E6: Authentication successful

Fig. 1

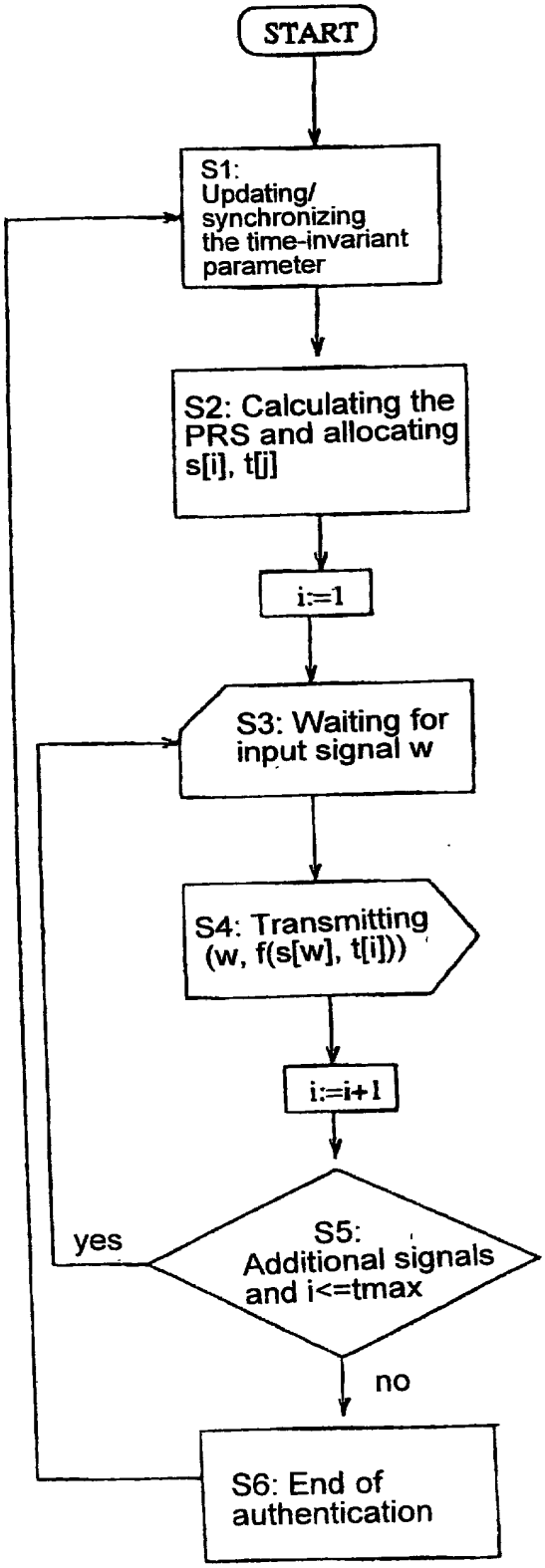
START
S1: Updating/ synchronizing the time-invariant parameter
S2: Calculating the PRS and allocating s[i], t[j]
i:=1
S3: Waiting for input signal w
S4: Transmitting (w, f(s[w], t[i]))
i:=i+1
S5: Additional signals and i<=tmax
yes
no
S6: End of authentication

Fig. 2

P36024.P2

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	
DECLARATION AND POWER OF ATTORNEY	ATTORNEY'S DOCKET NO. **2345/62**

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name,

I believe I am an original, first, and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled **SIGNAL TRANSMISSION PROCESS** the specification of which was filed as International Application No. PCT/EP97/05081 on September 17, 1997.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

PRIOR FOREIGN APPLICATION(S)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119
GERMANY	**196 40 526.2**	**01 October 1996**		**YES**

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys:
Richard L. Mayer (Reg. No. ~~22,490~~)
William C. Gehris (Reg. No. ~~38,156~~)
Erik R. Swanson (Reg. No. ~~40,833~~)

SEND CORRESPONDENCE, AND DIRECT TELEPHONE CALLS TO:

Richard L. Mayer
KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (phone)
(212) 425-5288 (facsimile)

EL169614947US

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR	FAMILY NAME **SCHEERHORN**	FIRST GIVEN NAME **Alfred**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-49716 Meppen**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Ahornallee 3**	CITY **D-49716 Meppen**	STATE & ZIP CODE/COUNTRY **Germany**
Signature		Date	
FULL NAME OF INVENTOR	FAMILY NAME **HUBER**	FIRST GIVEN NAME **Klaus**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-64283 Darmstadt**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Ernst-Ludwig-Strasse 21**	CITY **D-64283 Darmstadt**	STATE & ZIP CODE/COUNTRY **Germany**
Signature		Date 11th march 1999	

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR	FAMILY NAME 3-00 **SCHEERHORN**	FIRST GIVEN NAME **Alfred**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-49716 Meppen** DE	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Ahornallee 3**	CITY **D-49716 Meppen**	STATE & ZIP CODE/COUNTRY **Germany**
Signature		Date	
FULL NAME OF INVENTOR	FAMILY NAME 4-00 **HUBER**	FIRST GIVEN NAME **Klaus**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-64283 Darmstadt** DE	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Ernst-Ludwig-Strasse 21**	CITY **D-64283 Darmstadt**	STATE & ZIP CODE/COUNTRY **Germany**
Signature Alfred Scheerhorn		Date 10.03.1999	